(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日:
2005年7月7日(07.07.2005)

PCT

(10) 国际公布号:
WO 2005/062546 A1

(51) 国际分类号[7]: H04L 12/56

(21) 国际申请号: PCT/CN2004/001516

(22) 国际申请日: 2004年12月24日(24.12.2004)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200310121080.8 2003年12月24日(24.12.2003) CN

(71) 申请人(对除美国以外的所有指定国): 华为技术有限公司(HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人;及
(75) 发明人/申请人(仅对美国): 袁莉(YUAN, Li) [CN/CN]; 严军(YAN, Jun) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京德琦知识产权代理有限公司(DEQI INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区花园东路10号高德大厦8层, Beijing 100083 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

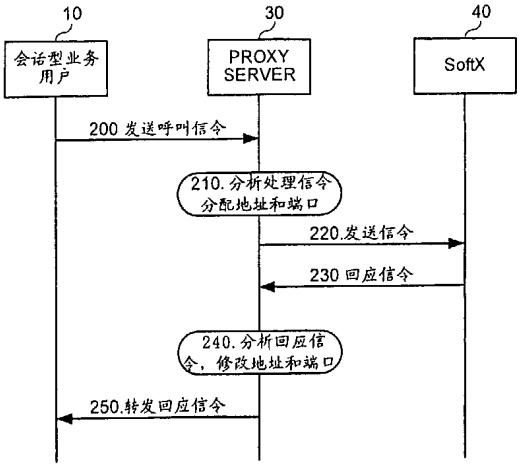
(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚专利(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲专利(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

本国际公布:
— 包括国际检索报告。

所引用双字母代码和其它缩写符号，请参考刊登在每期PCT公报期刊起始的"代码及缩写符号简要说明"。

(54) Title: A METHOD FOR ACHIEVING THE CONVERSION AND TRAVERSE OF NETWORK ADDRESS AND SYSTEM THEREOF

(54) 发明名称: 实现网络地址转换穿越的方法及其系统




10 SESSIONAL SERVICE SUBSCRIBER
30 PROXY SERVER
40 SOFTX
200 SENDING A CALL SIGNALING
210 ANALYZING AND MANAGING THE SIGNALING, ASSIGNING AN ADDRESS AND A PORT
220 SENDING THE SIGNALING
230 RESPONDING TO THE SIGNALING
240 ANALYZING THE RESPONSIVE SIGNALING MODIFYING THE ADDRESS AND THE PORT
250 TRANSMITTING THE RESPONSIVE SIGNALING

(57) **Abstract:** The invention relates to a method for achieving the conversion and traverse of network address. The invention adopts a means of FULL PROXY and achieves the traverse of the export network address transmitter (NAT)/ the firewall (FW) by relaying the call signaling and the media stream of the user terminal in the private network at the same time. Meantime, the invention further discloses a system for achieving the conversion and traverse of network address. Applying this invention, it doesn't need to modify the current NAT/FW and the user terminal when achieving traverse in the form of any configurable networks, and it can resolve the problems about Quality of Service (QoS), security and the aging of NAT mapping table at the same time.

WO 2005/062546 A1

[见续页]

(57) 摘要

本发明公开了一种实现网络地址转换穿越的方法，该方法采用全代理（FULL PROXY）方式，通过对私网内用户终端的呼叫信令和媒体流同时做中继来实现出口网络地址转换服务器（NAT）/防火墙（FW）的穿越。同时，本发明还公开了一种实现网络地址转换穿越的系统。应用本发明，在任何组网形式下实现穿越时均都不需要对现有的NAT/FW和用户终端进行改造，并可以同时解决服务质量（QoS）、安全以及NAT映射表老化的问题。

# 实现网络地址转换穿越的方法及其系统

## 技术领域

本发明涉及下一代网络（Next Generation Network，简称“NGN”）中通信技术领域，特别涉及 NGN 中实现网络地址转换穿越的方法及其系统。

## 发明背景

NGN 是电信史的一块里程碑，它标志着新一代电信网络时代的到来。从发展的角度来看，NGN 是从传统的以电路交换为主的公用电话交换网（Public Switched Telephone Network，简称“PSTN”）中逐渐迈出了向以分组交换为主的步伐，它承载了原有 PSTN 网络的所有业务，把大量的数据传输卸载到网间互联协议（Internet Protocol，简称“IP”）网络中以减轻 PSTN 网络的重荷，又以 IP 技术的新特性增加和增强了许多新老业务。从这个意义上讲，NGN 是基于时分多路复用（Time Division Multiplexing，简称“TDM”）的 PSTN 语音网络和基于网间互联协议/异步传输模式（IP/ATM）的分组网络融合的产物，它使得在新一代网络上语音、视频、数据等综合业务成为了可能。目前，NGN 成为了研究的热点。

NGN 在功能上可分为四个层次：接入和传输层、媒体传送层、网络控制层、网络服务层。软交换（SoftSwitch）为 NGN 提供具有实时性要求的业务的呼叫控制和连接控制功能，是 NGN 呼叫与控制的核心。软交换构件（SoftX）为 NGN 的网络控制层的关键构件，是提供综合业务和呼叫控制的设备。其主要作用包括：呼叫控制、信令网关、网关控制、

综合业务、增强业务等。

随着 NGN 网络逐步从实验走向商用，NGN 用户的接入问题越来越成为一个严重的问题。由于 NGN 是一个基于分组网承载的网络，接入用户都是通过 IP 地址来寻址，而当前网络由于 IP 地址紧缺以及安全等各种原因，大量的企业网和驻地网基本上都采用了私有 IP 地址通过出口的网络地址转换/防火墙（NAT/FW）接入公网。

然而，目前 NGN 中，在 IP 上承载诸如 H.323、会话初始协议（Session Initiationl Protocol ，SIP）、网关控制协议（Media Gateway Control Protocol ，MGCP）、H.248 等语音和视频协议时，由于报文的负载中有与报头不一样的地址，使得这些协议的控制通道/媒体通道难以穿越传统的 NAT/FW 设备与公网进行互通。其具体原因可通过对 NAT/FW 的分析得知：

防火墙，即 FW，用于限制数据包无限制的进入网络内。一般是设定一些包过滤原则，防火墙通过检查数据包的源地址、目标地址、源端口、目标端口和协议来判断数据包是否符合过滤原则，符合的数据包才可以通过防火墙。在实际应用时，通常将一些需要外界访问的服务器，如 Web 服务器等放在这个区域内，配置防火墙，使所有发往这些服务器的对应端口的数据包可以通过。在进行多媒体通信时，即使防火墙可以让最初建立呼叫的发往固定端口的数据包进入，由于音/视频通信需要通过动态分配端口来建立发送和接收数据的通道，其范围较大且无法事先预知内部终端的 IP 地址和端口信息，防火墙不可能不顾局域网的安全，开放这么大的包过滤范围。

另一方面，再从 NAT 考察有关原因：

NAT 用于隐藏局域网 IP 地址、保护局域网内主机不受外界攻击。由于局域网内的地址无法在公网上进行路由寻址，当数据包的目标地址

是 LAN 内地址时，数据包只能被丢弃掉。在进行多媒体通信时，如果 H.323 被叫方的地址是局域网地址，则该呼叫的数据包根本无法到达局域网内终端。当从局域网内向外发起呼叫时，呼叫方的 IP 地址，即局域网 IP 地址，和端口信息会加载在数据包的负载中，被叫方接收到数据包后，根据数据包负载中的源 IP 地址和端口发送音频、视频流，当这个 IP 地址是一个无法进行路由寻址的 IP 时，即上述局域网 IP 地址无法进行路由寻址的情况，Internet 上的路由器只能将这些数据包丢掉。因此，表面上看起来呼叫已经建立，但实际上在 NAT 内的终端是无法接收到外面终端的音频和视频的。另外，NAT 还通过网络地址/端口转换使局域网内的多个终端能够共享较少数量的公网 IP 地址。如在局域网内的某个终端执行某个应用时，将其局域网 IP 地址和端口映射成网关的外网 IP 地址和端口。在多媒体通信时，只有多媒体流通道是从内向外建立时，NAT 设备才可以建立对应的端口映射关系，传送到网关的外网 IP 地址上的多媒体流才可正确地传送到局域网的终端。如果多媒体流通道是从外向内建立的，则 NAT 设备无法建立映射关系，多媒体流的传送会失败。再有，如果这些通道采用的是超时的机制维持，如果在超时时间内该通道没有数据传送，这个映射关系就会被取消掉，在多媒体通信时，如果需要有很长时间停止通道上多媒体数据传送时，需要采取一定的措施来维持通道的建立。

上面详细分析了音频、视频业务无法通过 NAT/FW 的原因。然而，NGN 网络最大的好处之一就是能为用户提供丰富的业务，特别是为企业用户提供语音、数据、视频融合的业务，因此上面所提到问题的解决就更加的迫切，成为目前 NGN 网络业务开展最大的障碍。另一方面，宽带接入网络由于大多不属于运营商网络，运营商无法对其进行统一规划，使得接入网络的 IP 地址问题、业务质量保证（Quality of Service ，

简称“QoS”）和安全保证问题、实时会话业务和数据业务的区分等问题难以得到解决，这些问题成为困扰运营商的重要方面。

目前业界现有的解决方法有应用层网关方式（Application Layer Gateway，简称“ALG”）、中间盒通讯方式（Middlebox Communication，简称“MIDCOM”）、用户数据报协议（User Datagram Protocol，UDP）对 NAT 的简单穿越方式（Simple Traversal of UDP Through Network Address Translators，简称“STUN”）、通过中继方式穿越 NAT 方式（TURN）。

下面简单说明上述各种现有技术的内容。

第一种：ALG 方式。普通 NAT 是通过修改 UDP）或传输控制协议（Transfer Control Protocol，TCP）报文头部地址信息实现地址的转换，但部分承载于 TCP/UDP 的应用，如多媒体会话、文件共享、游戏等“端到端”的应用，在 TCP/UDP 负载中也需带地址信息。一般情况下，应用程序在 TCP/UDP 负载中填写自身地址，此地址信息在通过 NAT 时被修改为 NAT 上对外的地址，即我们常说的 ALG 方式。

ALG 功能目前主要驻留在一些 NAT/Firewall 设备中，要求这些设备本身具备应用程序识别的智能。同时每增加一种新的应用程序都需要对 NAT/Firewall 进行升级。

对 NGN 业务应用，ALG 需要支持 IP 语音和诸如 H323、SIP、MGCP/H.248 等视频协议的识别和对 NAT/Firewall 的控制，以使 NGN 业务顺利穿越。

ALG 的关键点为：企业网/驻地网内部终端能穿透 NAT/ALG 注册到公网 SoftX 上，通过 SoftX 进行协议解析和呼叫处理。公网 SoftX 和企业网终端通过 SIP/H.323/MGCP/H.248 协议互通，NAT/ALG 需要识别 SIP/ H.323/MGCP/H.248 协议信令并建立媒体流通道，以支持媒体流顺

利穿越 NAT/FW。

ALG 是支持 NGN 应用一种最简单的方式，但由于网络实际情况是已部署了大量不支持 NGN 业务应用的 NAT/FW 设备。

第二种情况：MIDCOM 方式。MIDCOM 与 ALG 不同，MIDCOM 的框架结构是采用可信的第三方 MIDCOM 代理（Agent）对中间盒（Middlebox） 进行控制的机制，应用业务识别的智能也由 Middlebox 转移到外部的 MIDCOM Agent 上，因此应用协议对 Middlebox 是透明的 。

由于应用业务识别的智能从Middlebox移到外部的MIDCOM Agent 上，根据 MIDCOM 的架构，在不需要更改 Middlebox 基本特性的基础上，通过对 MIDCOM Agent 的升级就可以支持更多的新业务，这是相对 ALG 方式的一个很大的优势。

在 NGN 业务实际应用中，Middlebox 功能可驻留在 NAT/FW，MIDCOM Agent 功能可驻留在 SoftX。通过软交换设备中的 MIDCOM Agent 对 IP 语音和诸如 H.323、SIP、MGCP/H.248 等视频协议的识别和对 NAT/ FW 的控制，它可以作为 NGN 业务穿越 NAT/FW 的一个解决方案。

MIDCOM 方式的关键点为：公网 SoftX 通过 MIDCOM 协议对私网边缘的 NAT/FW 设备进行控制，SoftX 识别主、被叫侧的 SIP/H323/MGCP/H248 协议，如主、被叫侧均为局内的私网用户，SoftX 需要通过 MIDCOM 协议控制主、被叫两侧的 NAT/FW，在 NAT/FW 上创建了媒体流通道后，媒体流可顺利穿越 NAT/FW。

由于软交换设备 SoftX 上已实现了对 SIP/H323/MGCP/H248 协议的识别，只需在 NAT/FW 设备上增加 MIDCOM 协议即可，而且以后新的应用业务识别随着软交换的支持而支持，因此这种方案是一种比较有前

途的解决方案，但现有的NAT/FW设备需升级支持MIDCOM协议。

第三种：STUN方式。解决NGN NAT问题的另一思路是，局域网内的用户终端通过某种机制预先得到其地址对应在出口 NAT 上的对外地址，然后在报文负载中所描述的地址信息就直接填写出口NAT上的对外地址，而不是该用户终端的在局域网内的IP地址，这样报文负载中的内容在经过NAT时就无需被修改了，只需按普通NAT流程转换报文头的IP地址即可，负载中的IP地址信息和报文头的IP地址信息又是一致的。STUN协议就是基于此思路来解决应用层地址的转换问题。

用户的应用程序，作为STUN客户端（CLIENT）向NAT外的STUN服务器（SERVER）通过UDP发送请求STUN消息，STUN SERVER收到请求消息，产生响应消息，响应消息中携带请求消息的源端口，即STUN CLIENT在NAT上对应的外部端口。然后，响应消息通过NAT发送给STUN CLIENT，STUN CLIENT通过响应消息体中的内容得知其在NAT上对应的外部地址，并且将其填入以后呼叫协议的UDP负载中，告知对端，本端的实时传输协议（RealTime Transfer Protocol ，RTP）接收地址和端口号为NAT外的地址和端口号。由于通过STUN协议已在NAT上预先建立媒体流的NAT映射表项，故媒体流可顺利穿越NAT。

STUN协议最大的优点是无需现有NAT/FW设备做任何改动。由于实际的网络环境中，已存在大量的NAT/FW，并且这些NAT/FW并不支持分组语音（Voice over IP，VoIP）的应用，如果用MIDCOM或NAT/ALG方式来解决此问题，需要替换现有的NAT/FW，这是不太容易的。而采用STUN方式无需改动NAT/FW，这是其最大优势，同时STUN方式可在多个NAT串联的网络环境中使用，但MIDCOM方式则无法实现对多级NAT的有效控制。

根据STUN原理，STUN SERVER必须放在公网中，可以内嵌在公

网 SoftX 中，由于通过 STUN 协议已在 NAT 上预先建立媒体流的 NAT 映射表项，故媒体流可顺利穿越 NAT。

STUN 的局限性在于需要应用程序支持 STUN CLIENT 的功能，即 NGN 的网络终端需具备 STUN CLIENT 功能。同时 STUN 并不适合支持 TCP 连接的穿越，因此不支持 H.323 应用协议。另外 STUN 方式还不支持 NGN 业务对防火墙的穿越，同时 STUN 方式不支持对称 NAT 类型的穿越。

第四种：TURN 方式。TURN 方式与 STUN 相似，其解决 NAT 问题的思路也是基于私网接入用户通过某种机制预先得到其私有地址对应在公网的地址，然后在报文负载中所描述的地址信息就直接填写该公网地址。不同的是，STUN 方式预先得到的地址为出口 NAT 上的地址，TURN 方式预先得到的地址为 TURN 服务器（SERVER）上的地址。

TURN 应用模型如图 1 所示，实现 TURN 方式的系统包括分组用户终端 10、11，NAT/FW 20、21，SoftX 40、41 以及 TURN SERVER50。它通过分配 TURN Server 的地址和端口作为 TURN 客户端（TURN CLIENT）对外的接受地址和端口，即局域网内用户终端发出的报文都要经过 TURN SERVER 进行中继转发。值得指出，这正是 STUN 方式与 TURN 方式区别最大的地方。这种方式除了具有 STUN 方式的优点外，还能解决 STUN 方式中应用无法穿透对称 NAT（Symmetric NAT）以及防火墙设备的缺陷，即无论企业网/驻地网出口为哪种类型的 NAT/FW，都可以实现 NAT 的穿透，同时 TURN 支持基于 TCP 的应用，如 H.323 协议。此外 TURN SERVER 控制分配地址和端口，能分配实时传输协议（RealTime Transfer Protocol，简称“RTP”）/实时传输控制协议（RealTime Transfer Control Protocol，简称“RTCP”）地址对作为本端客户的接受地址，其中 RTCP 端口号为 RTP 端口号加 1，从而避免了

STUN 应用模型下出口 NAT 对 RTP/RTCP 地址端口号的任意分配，使得客户端无法收到对端发过来的 RTCP 报文。

TURN 的局限性在于需要终端支持 TURN CLIENT，这一点同 STUN 一样对网络终端有要求。此外，所有报文都必须经过 TURN SERVER 转发，增大了包的延迟和丢包的可能性。

综上所述，上述四种方案分别存在以下问题：

对于 ALG 方式，不但需要对现有的大量 NAT/FW 进行改造以支持 ALG，而且 NAT/FW 此时难以支持业务的变化，还有因为 ALG 不能识别加密后的报文内容，所以必须保证报文采用明文传送，这使得报文在公网中传送时有很大的安全隐患。

对于 MIDCOM 方式，需要对现有大量的 NAT/FW 进行升级以支持 MIDCOM。而且，运营商难以对属于企业的 NAT/FW 进行升级和管理。

对于 TURN 方式，需要 NGN 的网络终端具备 TURN Client 功能，此外如果多媒体终端的信令收端口和发端口不一致，RTP/RTCP 的收端口和发端口不一致则可能造成无法穿越 NAT 的问题。

对于 STUN 方式，除了具有与 TURN 一样的问题，即需要网络终端支持和会因端口配置不一致而无法穿越 NAT 外，还不支持 TCP 连接穿越和对称 NAT 的穿越。

造成上述些缺点的主要原因在于，一方面，ALG、MIDCOM、STUN、TURN 方式的实现需要 NAT/FW 或用户终端的支持；另一方面，由于各种方式本身的缺陷，使得它们在面对一些应用无能为力。

## 发明内容

有鉴于此，本发明的主要目的在于提供一种实现网络地址转换穿越的方法及其系统，使得在任何组网形式下实现穿越时均不需要对现有的

NAT/FW 和用户终端进行改造。

为实现上述目的，本发明提供了一种实现网络地址转换穿越的方法，包含以下步骤：

A 当网络地址转换服务器或防火墙以外的代理服务器收到来自第一网络内分组用户终端的信令报文时，对该信令报文负载信息进行解析，记录该报文负载中的呼叫信令地址和端口，以及媒体流实时传输协议和实时传输控制协议地址和端口，并且将该报文负载信息中的呼叫信令地址和端口修改为所述代理服务器为该呼叫分配的在第二网络中的呼叫信令地址和端口，将该报文负载信息中的媒体流实时传输协议和实时传输控制协议地址和端口修改为所述代理服务器为该媒体流分配的在第二网络中的地址和端口；

B 所述代理服务器将修改后的所述信令报文发送到分组语音信令处理设备或业务处理设备；

C 当所述代理服务器收到发向所述第一网络内分组用户终端的回应信令报文时，对该回应信令报文负载信息进行解析，将该报文负载信息中回应信令地址和端口修改为步骤 A 中所记录的呼叫信令地址和端口，将该报文负载信息所携带的媒体流实时传输协议和实时传输控制协议地址和端口，修改为步骤 A 中所记录的媒体流实时传输协议和实时传输控制协议地址和端口；

D 所述代理服务器将修改后的所述回应信令报文发向所述第一网络内分组用户终端。

在步骤 A 之前，该方法可以进一步包括：

第一网络内的分组用户终端向所述代理服务器发送信令报文，该信令报文先被发送到网络地址转换服务器或防火墙，网络地址转换服务器或防火墙为该信令报文分配公网地址/端口，并将该信令报文 IP 头的源

地址从第一网络的地址/端口修改为为其分配的公网地址/端口，并在信令地址映射关系中记录所述第一网络地址/端口与网络地址转换服务器或防火墙分配的公网地址/端口之间的对应关系，然后把该信令报文转发到所述代理服务器。

在执行步骤 A 后，可以包括:

所述代理服务器定期向所述第一网络内分组用户终端发起报文，刷新所述网络地址转换服务器或防火墙上的信令地址映射关系。

步骤 A 还可以进一步包括:

当所述代理服务器收到来自所述第一网络内分组用户终端的呼叫信令时，记录该呼叫信令的报文 IP 头地址和端口，并将其修改为所述代理服务器为该呼叫分配的在第二网络中的呼叫信令地址和端口;

则步骤 C 进一步包括:

当所述代理服务器收到发向所述第一网络内分组用户终端的呼叫信令时，将该呼叫信令的报文 IP 头地址和端口修改为所述被记录的呼叫信令的报文 IP 头地址和端口。

其中，所述分组语音信令处理设备或业务处理设备是软交换设备或 IP 语音网守设备。

本发明提供的一种实现网络地址转换穿越的系统包含:

位于第一网络内分组用户终端，用于发起和接收业务;

位于第二网络内的代理服务器，用于接收来自第一网络的所述分组用户终端的信令报文，对该信令报文的报文负载信息进行解析，记录该报文负载中的呼叫信令地址和端口，以及媒体流地址和端口，并且将该报文负载中的呼叫信令地址修改为所述代理服务器为该呼叫分配的在第二网络中的呼叫信令地址和端口，将该报文负载中的媒体流地址和端口修改为所述代理服务器为该媒体流分配的在第二网络中的地址和端

口，然后将修改后的所述信令报文发送到所述软交换设备，和，当所述代理服务器收到发向所述第一网络内分组用户终端的回应信令时，对该回应信令的报文负载信息进行解析，将该报文负载中回应信令地址和端口修改为所述被记录的呼叫信令地址和端口，将该报文负载所携带的媒体流地址和端口，修改为所述被记录的媒体流地址和端口，然后将修改后的所述回应信令发向所述第一网络内分组用户终端；

软交换设备，用于提供综合业务和呼叫控制，在收到发送给所述分组用户终端的回应信令报文时转发给所述代理服务器。

该系统可以进一步包括：

网络地址转换服务器或防火墙，用于为所述分组用户终端提供接入第二网络的服务，为所述分组用户终端和所述代理服务器相互转发报文。

所述分组用户终端可以是使用 H.323 协议、或会话初始化协议、或媒体网关控制协议、或 H.248 协议进行音频和视频通信的用户终端。

所述代理服务器还可以用于按照流量计费。

所述代理服务器还可以用于用户的接入控制、带宽管理，对媒体流的服务质量标记、虚拟专用网标记和信息进行加密。

所述代理服务器还用于多个第一网络和第二网络地址对的设置，同时实现对多个网络地址转换服务器或防火墙的穿越。

对于媒体流的交互，所述代理服务器还可以采用首包刷新方式来更新媒体流的会话表项或地址转换关系表项。

通过比较可以发现，本发明的技术方案与现有技术的区别在于，本发明通过代理服务器对 NAT/FW 进行穿越，代理服务器不但对报文 IP 头的地址/端口进行转换，而且对报文中携带的信令地址/端口以及 RTP/RTCP 地址/端口也进行转换。

这种技术方案上的区别，带来了较为明显的有益效果，即该方案不需要 NAT/FW 设备进行任何改造；对业务终端没有需求，不需要终端修改；可以实现多层 NAT 和对称 NAT 的穿越；能同时实现对多个企业网/驻地网出口 FW/NAT 的穿越；提供用户的接入控制功能，提供对媒体流的 QoS 标记和信息加密，解决接入网络中实时会话业务的 QoS 保证和安全问题；而且还具有刷新 NAT 映射表和流量计费的功能。

## 附图简要说明

图 1 是 TURN 方式下的系统结构图；

图 2 是根据本发明的一个实施例的 FULL PROXY 方式的系统结构图；

图 3 是根据本发明的一个实施例的 FULL PROXY 方式的实现 NAT/FW 穿越的方法流程。

## 实施本发明的方式

为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述。

本发明采用全代理（FULL PROXY）方式，通过对私网内用户终端的呼叫信令和媒体流同时做中继来实现出口 NAT/FW 的穿越。

图 2 所示为实现本发明 FULL PROXY 方式的系统的一个具体实施例的结构示意图。为突出本发明，图 2 中只标出与本发明有密切关系的部分。

如图 2 所示，本实施例的系统包括分组用户终端 10 和 11、NAT/FW 20 和 21、代理服务器（PROXY SERVER）30、软交换设备（SoftX）40

和 41。其中，分组用户终端 10、11 分别属于不同的网络，分别通过 NAT/FW 20、21 与 PROXY SERVER30 相连; PROXY SERVER30 与 SoftX 40、41 相连。图中实线为媒体流，虚线为信令流。

分组用户终端 10、11 是指使用诸如 H.323、会话初始化协议( Session Initation Protocol，SIP )、媒体网关控制协议（Media Gateway Control Protocol， MGCP )、H.248 等音频/视频协议通信的用户终端。分组用户终端是多媒体业务的发起者和接收者，在私网中，分别通过 NAT/FW20 和 21 接入公网。需要指出的是，本发明中提到的私网和公网只是一个具体的特例，实质上只要是两个网络都可以，可以是不同的局域网，也可以一个是局域网，一个为外部公共网络，只要一个网络在 NAT/FW 之内，即认为该网络为私网，另一个网络在 NAT/FW 之外，即认为该网络为公网。

NAT/FW 20、21 是指实现 NAT 功能和防火墙功能的设备，通常配置在私网接入公网的位置。它一方面用于防止数据包无限制的进入私网内，保护私网内主机不受外界攻击；另一方面通过网络地址端口转换，隐藏私网 IP 地址，使私网内的多个用户终端能够共享较少数量的公网 IP 地址。

PROXY SERVER 30 类似于现有技术中的 TURN SERVER，置于城域网汇聚层，用于实现 FULL PROXY 的功能，即信令代理以及媒体中继功能。具体功能如下：PROXY SERVER30 在收到来自分组用户终端 10 的信令报文时，对信令报文负载进行解析与处理，得到该信令报文的 IP 头地址/端口、该信令报文负载中的呼叫信令地址/端口以及该用户终端接收媒体流地址/端口，这些地址/端口为私网地址/端口。并且，PROXY SERVER30 在公网中分别为该信令报文、该信令报文的负载中的呼叫信令以及该用户终端接收媒体流分配呼叫信令地址/端口。并记录上述私网

地址/端口与公网地址/端口的对应关系。

然后，将信令报文的 IP 头地址/端口修改为 PROXY SERVER30 为该呼叫分配的在公网中的信令报文地址/端口，将该信令报文负载中的呼叫信令地址修改为 PROXY SERVER30 为该呼叫分配的在公网中地址/端口，将该信令报文负载中的媒体流地址/端口修改为 PROXY SERVER30 为该媒体流分配的在公网中的地址/端口。然后将经过地址修改的信令报文发送到 SoftX 40、41。当 PROXY SERVER30 收到来自 SoftX 40、41 发向分组用户终端 10 的信令报文时，根从自身记录的对应关系中获取该信令报文的 IP 头地址/端口对应的私网内的 IP 头地址/端口，该信令报文负载中呼叫信令地址/端口所对应的私网内的呼叫信令地址/端口，以及该信令报文负载中媒体流的地址/端口所对应的私网内的媒体流的地址/端口，将该信令报文的 IP 头地址/端口修改为私网中信令报文 IP 头地址/端口；将该信令报文负载中呼叫信令地址/端口修改私网中的呼叫信令地址/端口；将该信令报文所携带的媒体流地址/端口修改为私网中的媒体流地址/端口；最后，按照修改后的信令报文 IP 头地址对该报文进行转发。这样，呼叫信令以及媒体流就可以通过 PROXY SERVER30 在主被叫之间进行中转。

熟悉本发明领域的技术人员会理解，PROXY SERVER30 可以配置多个 IP 地址对。如果 PROXY SERVER30 上配置有多个私网的 IP 地址或多个公网 IP 地址，则可以用一台设备同时实现对多个企业网/驻地网出口 FW/NAT 的穿越或同时代理多个软交换。通过这种方式确保了 PROXY SERVER30 无论在哪种组网模式，无论 NAT 是否对称 NAT，媒体流都能得到正确转发。

此外，通过对信令的处理和分析，PROXY SERVER30 不仅得到本次会话的地址变换情况，还可以获得带宽需求等服务质量（Quality of

Service，简称“QoS”）信息。由此，它能通过会话状态信息来控制媒体流的通过与关闭，起到保护网络、防范带宽盗用等。PROXY SERVER30可以提供对用户的接入控制功能、带宽管理功能，提供对媒体流的QoS标记、虚拟局域网（Virtual Local Area Network，简称“VLAN”）标记和信息加密。

为了防止NAT映射表老化问题，本发明还可以引入NAT地址绑定关系的定时刷新机制，即PROXY SERVER30在信令解析获得地址后就定期向分组用户终端10发起报文，来刷新企业出口NAT/FW20上的信令地址映射关系，即私网IP地址/端口与NAT/FW20分配的公网上的IP地址/端口的对应关系。在解决信令地址对企业出口NAT的穿越后，对于媒体流的交互，PROXY SERVER30采用首包刷新方式来更新媒体流的会话表项或地址转换关系表项，即在终端发出媒体流后，经过企业出口的NAT/FW20进行转换到达PROXY SERVER30，通过首包学习得到出口NAT/FW20上动态分配的地址/端口信息，从而更新媒体流会话表项，建立一个完整的媒体流会话表项，完成位于公网接入多个企业时的媒体转发功能。

在系统中引入PROXY SERVER30后，由于主叫方和被叫方的媒体流都经过PROXY SERVER30，所以PROXY SERVER30可以准确地获得媒体流量，从而实现基于报文流量的计费，而不仅仅是传统的基于时长的计费。

SoftX40、41是软交换设备，作为NGN的网络控制层的关键构件，用于提供综合业务和呼叫控制。在收到公网发送给私网中的分组用户终端的信令报文时，将收到的该报文转发给PROXY SERVER30。

下面再具体说明本发明中的基于FULL PROXY方式的穿越NAT/FW的方法流程。

作为本发明的一个较佳实施例，假设由分组用户终端 10 发起相关业务到分组用户终端 11，过程如图 3 所示：

步骤 200: 私网内的分组用户终端 10 向 PROXY SERVER30 发送信令报文，该信令报文中包含注册和呼叫信息，并且该信令报文的 IP 头的源地址为私网地址。分组用户终端 10 将 PROXY SERVER30 看作软交换设备。具体地说，源自分组用户终端 10 的信令报文先被发送到 NAT/FW 20，NAT/FW 20 为该信令报文分配一个公网地址/端口，并将其报文 IP 头的源地址从私网地址/端口修改为为其所分配的公网地址/端口，但是对报文内部信息不作任何改动，记录上述私网地址/端口与 NAT/FW 20 分配的公网地址/端口之间的对应关系，然后把该信令报文转发到 PROXY SERVER30。

步骤 210: 当 PROXY SERVER30 收到该信令报文后，对该信令报文负载中携带的信息进行解析与处理，得到信令报文的 IP 头地址/端口、报文负载中的呼叫信令地址/端口以及用户终端所请求的媒体流地址/端口，并且，PROXY SERVER30 为该信令报文、该信令报文负载中的呼叫信令以及该用户终端所请求的媒体流分别分配在公网中的地址/端口。然后，PROXY SERVER30 将信令报文 IP 头地址/端口修改为 PROXY SERVER30 为该呼叫分配的在公网中的地址/端口，将该报文负载中的呼叫信令地址修改为 PROXY SERVER30 为该呼叫分配的在公网中的呼叫信令地址/端口，将该报文负载中的媒体流地址/端口修改为 PROXY SERVER30 为该媒体流分配的在公网中的地址/端口，并记录私网内的信令报文的 IP 头地址/端口、报文负载中的呼叫信令地址/端口以及用户终端所请求的媒体流地址/端口与 PROXY SERVER30 分配的公网内的地址/端口之间的对应关系。

步骤 220: 将步骤 210 中修改后的信令报文转发给软交换设备

SoftX40。

步骤 230: 当 SoftX40 收到需要发向分组用户终端 10 的回应信令报文时，将该回应信令报文转发给 PROXY SERVER30。

步骤 240: PROXY SERVER30 收到发向私网内分组用户终端 10 的回应信令报文时，对该回应信令报文负载信息进行解析，得到回应信令报文的 IP 头地址/端口、回应信令报文负载中回应信令的地址/端口、媒体流地址/端口，然后根据回应信令报文的 IP 头地址/端口、回应信令报文负载中回应信令的地址/端口 、媒体流地址/端口从自身记录的对应关系中获取对应的私网中 IP 地址、呼叫信令地址/端口、媒体流地址/端口，然后将该回应信令报文的 IP 头地址/端口修改为私网中对应的 IP 头地址/端口，将该回应信令报文负载中回应信令地址/端口修改为私网中对应的呼叫信令地址/端口，将该回应信令所携带的媒体流地址/端口，修改为私网中对应的媒体流地址/端口。这里，媒体流地址/端口可以为 RTP/RTCP 地址/端口。

通过在步骤210和步骤240中对报文负载中信令和媒体流地址/端口的记录和修改，实现了对 NAT/FW 的穿越，并且在任何组网形式下实现穿越时均不需要对现有的 NAT/FW 和用户终端进行改造。

步骤 250: PROXY SERVER30 将修改后的回应信令报文发向私网内分组用户终端 10。

具体地说，PROXY SERVER30 首先将修改后的回应信令报文发送给 NAT/FW20，该报文的目的地址是 NAT/FW20 为分组用户终端 10 的呼叫分配的公网地址/端口，NAT/FW20 从自身记录的私网地址/端口和公网地址/端口的对应关系表中查询出该报文的公网目的地址/端口所对应的私网地址/端口，然后用查询到的私网地址/端口替换该报文的公网目的地址/端口，然后将经过地址/端口转换的回应信令报文转发给分组

用户终端 10。

从上述过程可以看出，本发明的 FULL PROXY 方式与 TURN 方式的中继相比，有如下区别：

TURN 方式是在 TURN SERVER 与用户终端通过 TURN 协议交互时分配地址/端口，报文内部的地址信息由终端生成，TURN SERVER 对后续的报文根据分配的地址/端口信息进行地址变换后中继转发。而 FULL PROXY 方式是通过对报文进行中继的设备对呼叫协议解析与处理，改写报文其中携带的媒体流地址信息后转发信令报文，同时根据改写的媒体流地址信息对媒体报文做地址变换后中继转发。

虽然通过参照本发明的某些优选实施例，已经对本发明进行了图示和描述，但本领域的普通技术人员应该明白，可以在形式上和细节上对其作各种各样的改变，而不偏离所附权利要求书所限定的本发明的精神和范围。

# 权利要求书

1、一种实现网络地址转换穿越的方法，其特征在于，该方法包含以下步骤:

A 当网络地址转换服务器或防火墙以外的代理服务器收到来自第一网络内分组用户终端的信令报文时，对该信令报文负载信息进行解析，记录该报文负载中的呼叫信令地址和端口，以及媒体流实时传输协议和实时传输控制协议地址和端口，并且将该报文负载信息中的呼叫信令地址和端口修改为所述代理服务器为该呼叫分配的在第二网络中的呼叫信令地址和端口，将该报文负载信息中的媒体流实时传输协议和实时传输控制协议地址和端口修改为所述代理服务器为该媒体流分配的在第二网络中的地址和端口;

B 所述代理服务器将修改后的所述信令报文发送到分组语音信令处理设备或业务处理设备;

C 当所述代理服务器收到发向所述第一网络内分组用户终端的回应信令报文时，对该回应信令报文负载信息进行解析，将该报文负载信息中回应信令地址和端口修改为步骤 A 中所记录的呼叫信令地址和端口，将该报文负载信息所携带的媒体流实时传输协议和实时传输控制协议地址和端口，修改为步骤 A 中所记录的媒体流实时传输协议和实时传输控制协议地址和端口;

D 所述代理服务器将修改后的所述回应信令报文发向所述第一网络内分组用户终端。

2、根据权利要求 1 所述的方法，其特征在于，在步骤 A 之前进一步包括:

第一网络内的分组用户终端向所述代理服务器发送信令报文，该信

令报文先被发送到网络地址转换服务器或防火墙，网络地址转换服务器或防火墙为该信令报文分配公网地址/端口，并将该信令报文 IP 头的源地址从第一网络的地址/端口修改为为其分配的公网地址/端口，并在信令地址映射关系中记录所述第一网络地址/端口与网络地址转换服务器或防火墙分配的公网地址/端口之间的对应关系，然后把该信令报文转发到所述代理服务器。

3、根据权利要求 1 所述的方法，其特征在于，在执行步骤 A 后，包括:

所述代理服务器定期向所述第一网络内分组用户终端发起报文，刷新所述网络地址转换服务器或防火墙上的信令地址映射关系。

4、根据权利要求 1 所述的方法，其特征在于，所述分组语音信令处理设备或业务处理设备是软交换设备或 IP 语音网守设备。

5、根据权利要求 1 所述的方法，其特征在于，步骤 A 还进一步包括:

当所述代理服务器收到来自所述第一网络内分组用户终端的呼叫信令时，记录该呼叫信令的报文 IP 头地址和端口，并将其修改为所述代理服务器为该呼叫分配的在第二网络中的呼叫信令地址和端口;

则步骤 C 进一步包括:

当所述代理服务器收到发向所述第一网络内分组用户终端的呼叫信令时，将该呼叫信令的报文 IP 头地址和端口修改为所述被记录的呼叫信令的报文 IP 头地址和端口。

6、一种实现网络地址转换穿越的系统，其特征在于，该系统包含:

位于第一网络内分组用户终端，用于发起和接收业务;

位于第二网络内的代理服务器，用于接收来自第一网络的所述分组用户终端的信令报文，对该信令报文的报文负载信息进行解析，记录该

报文负载中的呼叫信令地址和端口，以及媒体流地址和端口，并且将该报文负载中的呼叫信令地址修改为所述代理服务器为该呼叫分配的在第二网络中的呼叫信令地址和端口，将该报文负载中的媒体流地址和端口修改为所述代理服务器为该媒体流分配的在第二网络中的地址和端口，然后将修改后的所述信令报文发送到所述软交换设备，和，当所述代理服务器收到发向所述第一网络内分组用户终端的回应信令时，对该回应信令的报文负载信息进行解析，将该报文负载中回应信令地址和端口修改为所述被记录的呼叫信令地址和端口，将该报文负载所携带的媒体流地址和端口，修改为所述被记录的媒体流地址和端口，然后将修改后的所述回应信令发向所述第一网络内分组用户终端；

软交换设备，用于提供综合业务和呼叫控制，在收到发送给所述分组用户终端的回应信令报文时转发给所述代理服务器。

7、根据权利要求 6 所述的系统，其特征在于，该系统进一步包括：

网络地址转换服务器或防火墙，用于为所述分组用户终端提供接入第二网络的服务，为所述分组用户终端和所述代理服务器相互转发报文。

8、根据权利要求 6 所述的系统，其特征在于，所述分组用户终端是使用 H.323 协议、或会话初始化协议、或媒体网关控制协议、或 H.248 协议进行音频和视频通信的用户终端。

9、根据权利要求 6 所述的系统，其特征在于，所述代理服务器还用于按照流量计费。

10、根据权利要求 6 所述的系统，其特征在于，所述代理服务器还用于用户的接入控制、带宽管理，对媒体流的服务质量标记、虚拟专用网标记和信息进行加密。

11、根据权利要求 6 所述的系统，其特征在于，所述代理服务器还

用于多个第一网络和第二网络地址对的设置，同时实现对多个网络地址转换服务器或防火墙的穿越。

12、根据权利要求 6 所述的系统，其特征在于，所述代理服务器采用首包刷新方式来更新媒体流的会话表项或地址转换关系表项。

5

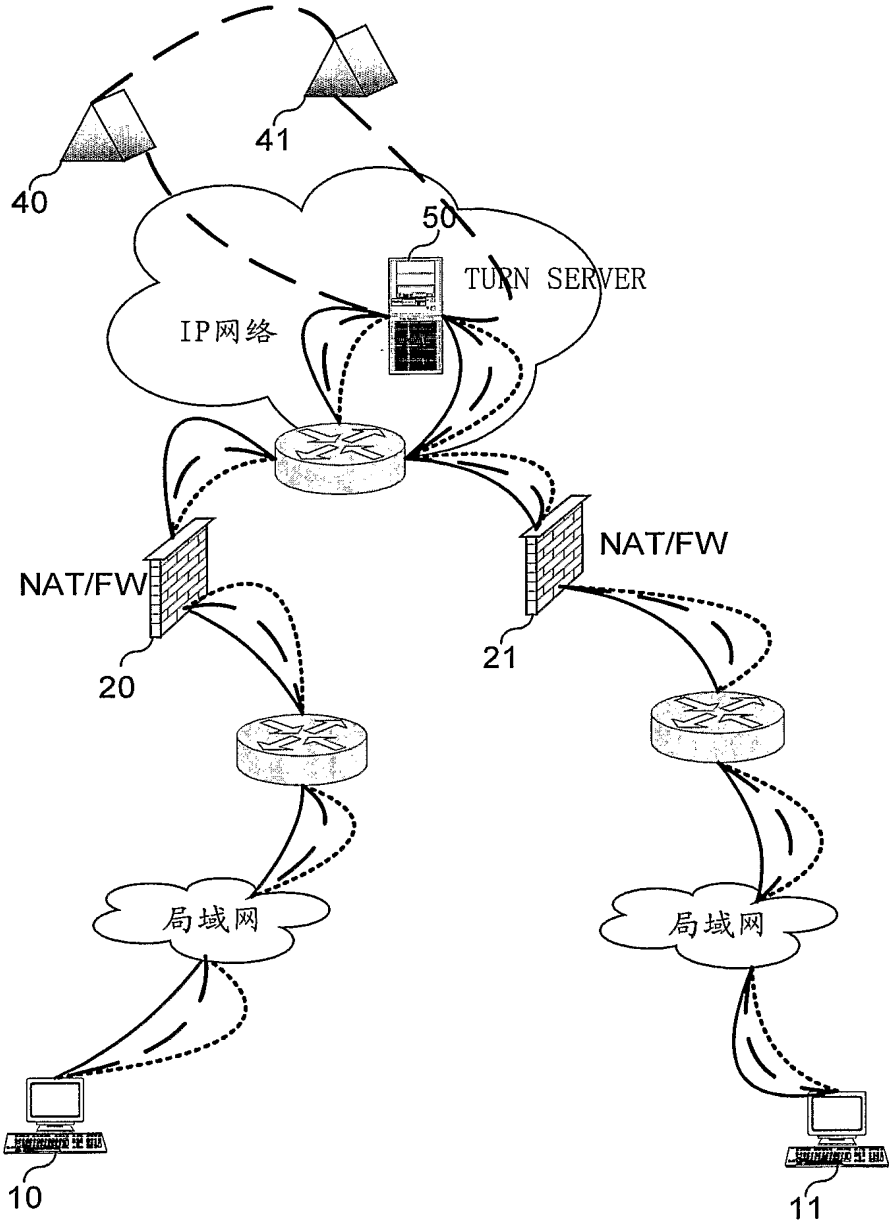



图 1

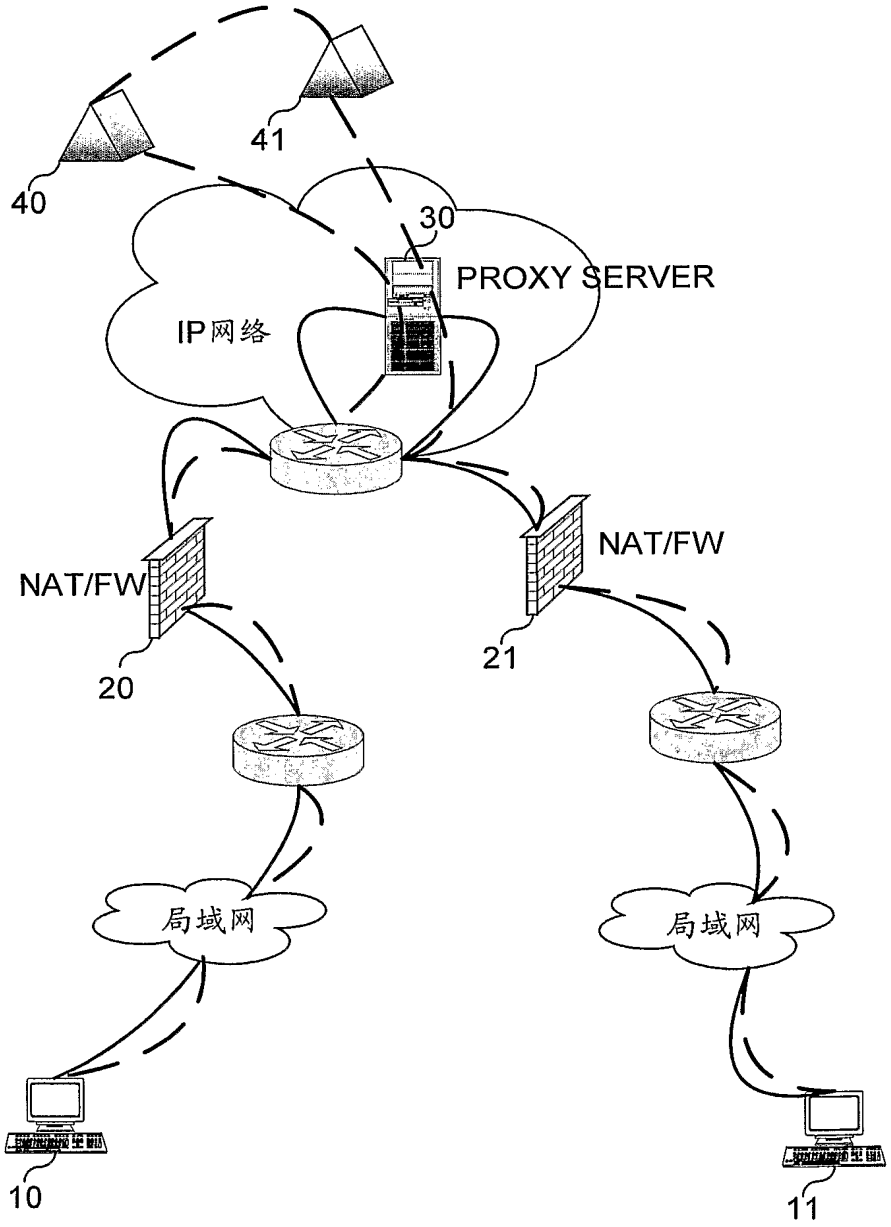



图 2

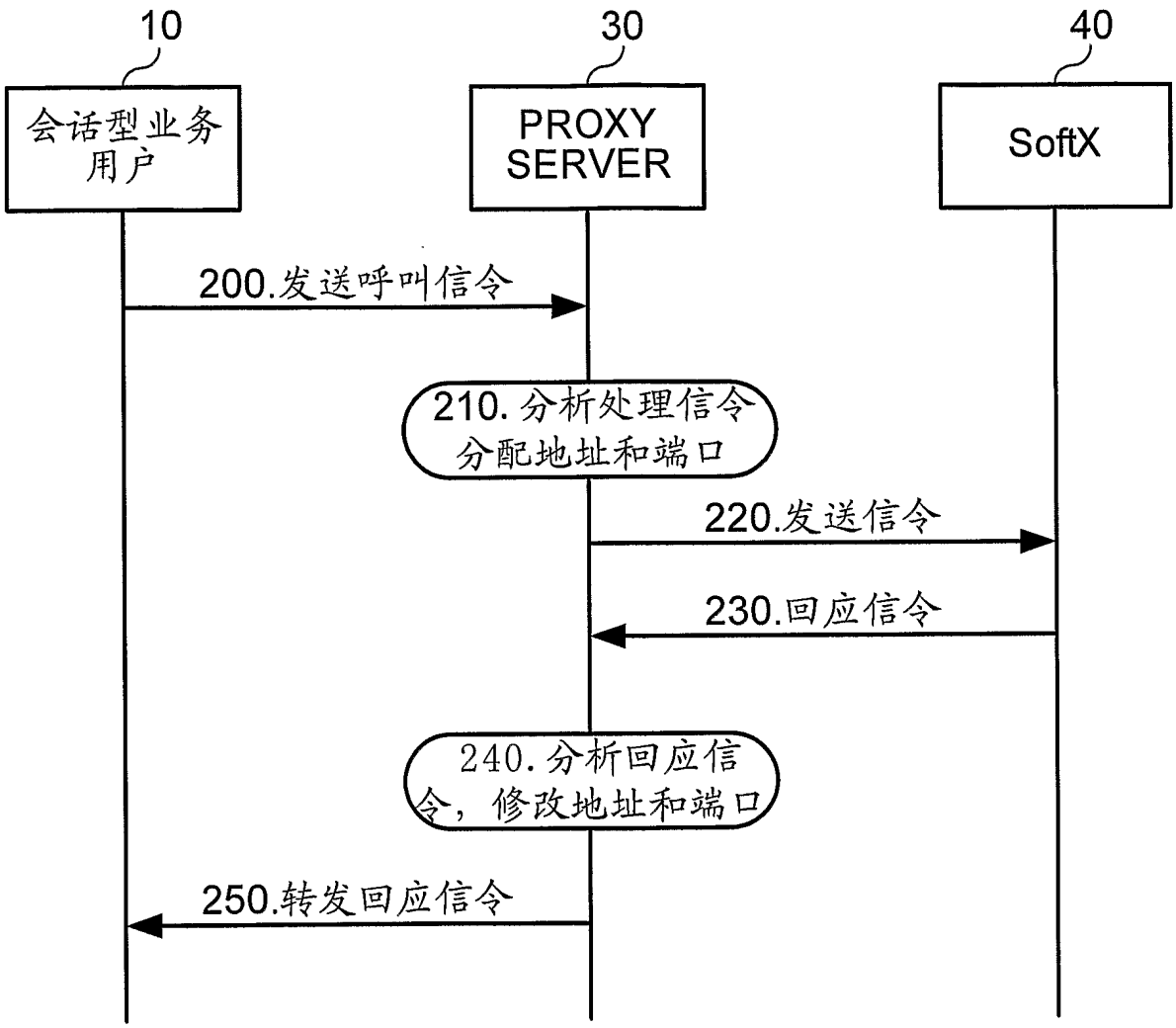

10
30
40
会话型业务用户
PROXY SERVER
SoftX
200.发送呼叫信令
210.分析处理信令分配地址和端口
220.发送信令
230.回应信令
240.分析回应信令，修改地址和端口
250.转发回应信令

图 3

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2004/001516

A. CLASSIFICATION OF SUBJECT MATTER

IPC[7] H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7] H04L12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, PAJ, CNPAT

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | US,A1,20030048780 (PHOMSOPHA B K) 13 Mar 2003 (13.03.03), see the whole document and figure 1-14 | 1—12 |
| A | CN,A,1411220 (HUAWEI TECHNOLOGIES CO.,LTD.) 16 Apr 2003 (16.04.03), see the whole document and figure 1-3 | 1—12 |

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
14 Mar 2005 (14. 03. 2005)

Date of mailing of the international search report
31 · MAR 2005 (31 · 03 · 2005)

Name and mailing address of the ISA/
6 Xitucheng Rd., Jimen Bridge, Haidian District,
100088 Beijing, China
Facsimile No. 86-10-62019451

Authorized officer
Sun Zhiling

Telephone No. (86-10)62084627

Form PCT/ISA /210 (second sheet) (January 2004)

**INTERNATIONAL SEARCH REPORT**
Information on patent family members

International application No.
PCT/CN2004/001516

| | | | |
|---|---|---|---|
| US2003048780A | 2003-03-13 | None | |
| CN1411220A | 2003-04-16 | WO03030463A | 2003-04-10 |

| 国际检索报告 | PCT/CN2004/001516 |
|---|---|

**A.** 主题的分类

IPC[7] H04L12/56

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

**B.** 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC[7] H04L12/56

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

WPI，EPODOC，PAJ，CNPAT

**C.** 相关文件

| 类 型* | 引用文件，必要时，指明相关段落 | 相关的权利要求 |
|---|---|---|
| A | US,A1,20030048780（PHOMSOPHA B K）2003 年 03 月 13 日（13.03.03），说明书全文及图 1－14 | 1－12 |
| A | CN,A,1411220（华为技术有限公司）2003 年 04 月 16 日（16.04.03）,说明书全文以及图 1－3 | 1－12 |

☐ 其余文件在 C 栏的续页中列出。 ☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

| 国际检索实际完成的日期 | 国际检索报告邮寄日期 |
|---|---|
| 14．03 月 2005（14．03．2005） | 31 · 3月 2005 (31 · 03 · 2005) |
| 中华人民共和国国家知识产权局(ISA/CN)<br>中国北京市海淀区蓟门桥西土城路 6 号 100088<br>传真号： (86-10)62019451 | 受权官员 孙志玲<br>电话号码：(86-10)62084627 |

# 国际检索报告
关于同族专利的信息

PCT/CN2004/001516

| 检索报告中引用的专利文件 | 公布日期 | 同族专利 | 公布日期 |
|---|---|---|---|
| US2003048780A | 2003-03-13 | 无 | |
| CN1411220A | 2003-04-16 | WO03030463A | 2003-04-10 |